UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,917	12/07/2005	Thomas Rottschafer	DE030203US1	9587

65913 7590 10/17/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
NGUYEN, TRONG H	

ART UNIT	PAPER NUMBER
4148	

NOTIFICATION DATE	DELIVERY MODE
10/17/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/559,917	ROTTSCHAFER ET AL.	
	Examiner	Art Unit	
	TRONG NGUYEN	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☒ Claim(s) *11, 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 February 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/07/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application numbered 10559917 filed on 12/07/2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63**.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

4. The applicant's submitted drawings are acceptable for examination purposes.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 12/07/2005 is in compliance with the provisions of 37 C.R.R. 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

6. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The abstract of the disclosure is objected to because the abstract in the instant application exceeds the maximum 150 word limit and includes the legal phraseology of "means". Correction is required. See MPEP § 608.01(b).

7. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.

(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Objections

8. Claim **11** is objected to because of the following informalities: Claim **11** recites a method involving a series of steps however it is intended to be dependent on claim **1** which recites an apparatus. Applicant therefore should consider either amending claim **11** to be an independent claim or reconsider the claim language and its dependency. Appropriate correction is required.

9. Claim **17** is objected to because of the following informalities: Claim **17** recites "a method as claimed in claim 10" but claim **10** recites an apparatus not a method. Therefore, reconsideration of the claim language and its dependency is suggested. Appropriate correction is required.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim **1** recites the limitation "rounding key" in line 4. The term "rounding key" makes the claim vague and unclear as to what the applicant meant since "rounding" can mean a mathematical rounding process or the technical term generally used in the art, a key used in a round of encryption/decryption of a block cipher. For examining purposes, hereinafter "rounding key" will be considered as round key. Furthermore, claim **1**, last line recites "decoupled". This term also makes the claim vague and unclear as to what the applicant meant since applicant's disclosure page 2, lines 3-5 recites "access to the at least one rounding key generation means can thus take place only by means of sequence control or the at least one encryption/decryption means." However, this claim recites "the at least one encryption/decryption means and the at least one rounding key generation means are decoupled from one another" in lines 7-9. For examining purposes, hereinafter "decoupled" will be considered as not in direct data path.

Claim **3** recites the limitation "the same line physics" in line 5. There is insufficient antecedent basis for this limitation in the claim. Furthermore, this term makes the claim vague and unclear as to what the applicant meant. For examining purposes, hereinafter "the same line physics" will be considered as using a single bus.

Claim **7** recites the limitation "the modes of operation" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claims **8** and **15** recite the limitation "inactive phase" in last lines. The term "inactive" makes the claims vague and unclear as to what the applicant meant. For

examining purposes, hereinafter "inactive phase" will be considered as when encryption/decryption is not carried out.

Claim **9** and **16** recite the limitation "the time" in lines 2. There is insufficient antecedent basis for this limitation in these claims.

Claim **12** and **13** recite the limitation "the communication" in line 2. There is insufficient antecedent basis for this limitation in these claims.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims **1** and **4** are rejected under 35 U.S.C. 102(b) as being anticipated by Matsui US 5,261,003 (hereinafter "Matsui"). For examining purposes, interpretations of "rounding key" and "decoupled" as previously mentioned in section **Claim Rejections - 35 USC 112** will be used.

Regarding claim **1**, Matsui discloses "**Processor for encrypting and/or decrypting data**," as ["a data communication system with a data scrambling" (Col. 5, lines 44-45, Fig. 1)] "**wherein a control device**" [selector 24, selector 25, and step counter 26 (Fig. 1)] "**is connected to at least one encryption/decryption means**" [scramble processing means 33 (Fig. 1, Col. 5, line 65)] "**via at least one communication means**," [Fig. 1] "**the control device is connected to at least one**

rounding key generation means" [address calculating circuit 23 and magnification key latch 7 (Fig. 1)] "**via at least one further communication means**" [Fig. 1] "**the control device has at least one external key input,**" [the magnification key latch 7 supplies the selected extended key to the selector 25 (Col. 6, lines 12-14, Fig. 1)] "**the at least one encryption/decryption means has at least one external data input**" [plaintext 3 (Fig. 1), selector 25 outputs selected extended keys to all of the scramble processing blocks 9-11 in scramble processing means 33 (Col. 6, lines 14-15, 34-36, Fig. 1)] "**and at least one external data output,**" [scrambled text 4 (Fig. 1)] **"and the at least one encryption/decryption means and the at least one rounding key generation means are decoupled from one another"** [scramble processing means 33 and address calculating circuit 23 and magnification key latch 7 are not in direct data path (Fig. 1)].

Regarding claim **4**, Matsui discloses **"A processor as claimed in claim 1, characterized in that the control device comprises at least one storage means in which at least one rounding key generated by the at least one rounding key generation means can be temporarily stored"** as [the extended key latch 7 supplies the selected extended key to the selector 25 and the key is then transmitted to the processing block 9 (Col. 6, lines 12-15).]

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims **2-3** and **6-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of John L. Hennessy and David A. Patterson, Computer Architecture: A Quantitative Approach, 2nd ed., Morgan Kaufmann, January 1996 (hereinafter "Hennessy and Patterson").

Regarding claim **2**, Matsui discloses "**A processor as claimed in claim 1**," but does not specifically disclose "**characterized in that the at least one communication means comprises at least one request line, at least one release line and at least one data line and/or the at least one further communication means comprises at least one further request line, at least one further release line and at least one further data line.**"

However, Hennessy and Patterson disclose an asynchronous bus comprising a request line, an acknowledgement line, and a data line (Page 499, Fig. 6.11).

Hennessy and Patterson and Matsui are analogous art because they are in the same field of endeavor of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui by including an asynchronous bus as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to lengthen the bus without worrying about clock skew or synchronization problems (Hennessy and Patterson, Page 499, Par. 3, lines 1-3).

Regarding claim **3**, for examining purposes, interpretation of "the same line physics" as previously mentioned in section **Claim Rejections - 35 USC 112** will be used. Matsui discloses "**A processor as claimed in claim 1**," but does not specifically disclose "**characterized in that the at least one request line, the at least one release line and the at least one data line and/or the at least one further request line, the at least one further release line and the at least one further data line at least partially use the same line physics.**"

However, Hennessy and Patterson disclose an asynchronous bus comprising a request line, an acknowledgement line, and a data line (Page 499, Fig. 6.11).

Hennessy and Patterson and Matsui are analogous art because they are in the same field of endeavor of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui by including an asynchronous bus as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to lengthen the bus without worrying about clock skew or synchronization problems (Hennessy and Patterson, Page 499, Par. 3, lines 1-3).

Regarding claim **6**, Matsui discloses "**A processor as claimed in claim 1**," but does not specifically disclose "**characterized in that at least one handshake protocol is provided for communication of the control device with the at least one encryption/decryption means and/or with the at least one rounding key generation means.**"

However, Hennessy and Patterson disclose an asynchronous bus wherein "self-timed, handshaking protocols are used between bus sender and receiver" (Page 499, Par. 2, lines 1-2).

Hennessy and Patterson and Matsui are analogous art because they are in the same field of endeavor of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui by using handshaking protocols as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to lengthen the bus without worrying about clock skew or synchronization problems (Hennessy and Patterson, Page 499, Par. 3, lines 1-3).

Regarding claim **7**, Matsui discloses "**A processor as claimed in claim 1**," but does not specifically disclose "**characterized in that the modes of operation of the control device, of the at least one encryption/decryption means and of the at least one rounding key generation means are asynchronous with respect to one another.**"

However, Hennessy and Patterson disclose an asynchronous bus wherein "self-timed, handshaking protocols are used between bus sender and receiver" (Page 499, Par. 2, lines 1-2).

Hennessy and Patterson and Matsui are analogous art because they are in the same field of endeavor of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui by including an asynchronous bus as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to lengthen the bus without worrying about clock skew or synchronization problems" (Hennessy and Patterson, Page 499, Par. 3, lines 1-3).

15. Claim **5** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Tran US 5,919,251 (hereinafter "Tran").

Matsui discloses "**A processor as claimed in claim 4**," but does not specifically disclose "**characterized in that at least one rotating pointer is provided for access to the at least one storage means**."

However, Tran discloses a rotating pointer buffer for storing data in integrated circuits wherein a head pointer and a tail pointer are used to provide access (Col. 1, lines 51, 54-47, Fig. 1).

Tran and Matsui are analogous art because they are in the same field of endeavor of data storage.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify data communication system with a data scrambling of Matsui by including at least one rotating pointer to provide access to storage areas in selectors as described by Tran since rotating pointer structure is superior to shifting structure in terms of lowest area consumption and speed (Tran, Col. 2, lines 18-20, Table 1).

16. Claims **8**, **9**, **11**, **15**, and **16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Muratani et al US 2002/0021802 (hereinafter "Muratani").

Regarding claim **8**, for examining purposes, interpretation of "inactive phase" as previously mentioned in section **Claim Rejections - 35 USC 112** will be used. Matsui discloses "**A processor as claimed in claim 1**," but does not disclose "**characterized in that at least one dummy calculation and/or at least part of at least one previous rounding key calculation can be carried out by means of the at least one rounding key generation means during at least one inactive phase.**"

However, Muratani discloses an encryption apparatus, decryption apparatus and expanded key generation apparatus and method (Col. 2, Par. 0025, lines 1-3) wherein all expanded keys or round keys are generated and stored prior to a decryption process (Col. 2, Par. 0022, lines 3-4). Furthermore, Muratani also discloses that only part of the expanded keys generated is used for data randomizing (Col. 8, Par. 0185, and Fig. 12-15).

Muratani and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Matsui's data communication system with a data scrambling by having round key generation and/or dummy calculations (non-used expanded keys)

during an inactive phase as described by Muratani in order to be effective and safe against attack (Muratani, Col. 8, Par. 0185, line 3).

Regarding claim **9**, Matsui discloses "**A processor as claimed in claim 1**," but does not specifically disclose "**characterized in that the time between calculation and use of the at least one rounding key is variable.**"

However, Muratani discloses that the order in which the expanded keys are generated may be changed, for example, an earlier generated expanded key may be temporarily stored in a memory to be used later than a later generated expanded key (Fig. 15, Col. 9, Par. 0197, lines 4-5, Par. 0199, lines 1-3).

Muratani and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Matsui's data communication system with a data scrambling by having time between calculation and use of at least one round key be varied as described by Muratani in order to be effective and safe against attack (Muratani, Col. 8, Par. 0185, line 3).

Regarding claim **11**, Matsui discloses "**A method of encrypting and/or decrypting data using a processor as claimed in claim 1**," as [a data communication method with a data scrambling (Col. 4, lines 5-6)] "**wherein a) at least one initial key is read into a control device**," [the magnification key latch 7 supplies the selected extended key to the selector 25 (Col. 6, lines 12-14, Fig. 1)] "**b) external data are read into at least one encryption/decryption means**," [plaintext 3 (Fig. 1), selector 25

outputs selected extended keys to all of the scramble processing blocks 9-11 in scramble processing means 33 (Col. 6, lines 14-15, 34-36 Fig. 1)] "**c) at least one data word needed to calculate at least one rounding key is read from at least one storage means of the control device and transferred to at least one rounding key generation means**," [the less significant 4 bytes of plaintext data are input to the address calculating circuit 23 through the selector 24 (Col. 6, lines 6-8)] "**d) at least one rounding key is calculated on the basis of the at least one data word by means of the at least one rounding key generation means, transferred to the control device and stored in the at least one storage means**," [the address calculating circuit 23 calculates an address of an extended key to be selected on the basis of the input plaintext data and outputs the calculated address to the extended key latch 7 (Col. 6, lines 8-12, Fig. 1) and the extended key latch 7 supplies the selected extended key corresponding to the given address to selector 25 (Col. 6, lines 12-14, Fig. 1)] "**e) the at least one rounding key is transferred to the at least one encryption/decryption means**," [selector 25 outputs selected extended keys to scramble processing blocks 9-11 in scramble processing means 33 (Col. 6, lines 14-15, 34-36, Fig. 1)] "**f) the external data are encrypted or decrypted by means of the at least one encryption/decryption means using the at least one rounding key**" [scramble processing means 3 scrambles an input data by using an extended key to output a scrambled data (Col. 6, lines 15-17, 36-39, Fig. 1)] "**and the encrypted or decrypted data are made available at least one external data output**," [scrambled text 4 (Col. 6, lines 44-48, Fig. 1)] and "**g) steps b) to f) are repeated as often as necessary to**

encrypt or decrypt a set of external data." ["the same processing as described above is repeated predetermined times to produce scrambled text 4 (Col. 6, lines 44-48)].

Matsui does not specifically disclose "**rounding key is calculated recursively**."

However, Muratani discloses a key generation method wherein round keys are generated recursively on the basis of previous sub keys (Fig. 1).

Muratani and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Matsui's data communication system with a data scrambling to calculate round key recursively as described by Muratani in order to be effective and safe against attack (Muratani, Col. 8, Par. 0185, line 3).

Regarding claim **15**, for examining purposes, interpretation of "inactive phase" as previously mentioned in section **Claim Rejections - 35 USC 112** will be considered. Matsui in view of Muratani disclose "**A method as claimed in claim 11, characterized in that at least one dummy calculation and/or at least part of at least one previous rounding key calculation is carried out by means of the at least one rounding key generation means during at least one inactive phase**" as [With respect to this limitation, Muratani discloses an encryption apparatus, decryption apparatus and expanded key generation apparatus and method (Col. 2, Par. 0025, lines 1-3) wherein all expanded keys or round keys are generated and stored prior to a decryption process (Col. 2, Par. 0022, lines 3-4). Furthermore, Muratani also discloses that only part of the expanded keys generated is used for data randomizing (Col. 8, Par. 0185, and Fig. 12-

15). Thus, Muratani makes it obvious that round key generation and/or dummy calculations (non-used expanded keys) can be carried out during an inactive phase (when encryption/decryption is not carried out).]

Regarding claim **16**, Matsui in view of Muratani disclose "**A method as claimed in claim 11, characterized in that the time between calculation and use of the at least one rounding key is variable**" as [With respect to this limitation, Muratani discloses that the order in which the expanded keys are generated may be changed, for example, an earlier generated expanded key may be temporarily stored in a memory to be used later than a later generated expanded key (Fig. 15, Col. 9, Par. 0197, lines 4-5, Par. 0199, lines 1-3). Therefore, Muratani makes it obvious that the time between calculation and use of at least one expanded or round key is variable.]

17. Claim **10** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view Verbauwhede US 2003/0202658 (hereinafter "Verbauwhede").

Matsui discloses "**A processor as claimed in claim 1**," but does not specifically disclose "**characterized in that said processor is embodied so as to be an AES processor**."

However, Verbauwhede discloses AES architecture for encrypting or decrypting data (Col. 1, Par. 0007, line 1).

Verbauwhede and Matsui are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Matsui's data communication system with a data scrambling to be an AES architecture as described by Verbauwhede in order to achieve a high data rate (Verbauwhede, Col. 1, Par. 0006, lines 1-2).

18. Claims **12-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Muratani, and further in view of Hennessy and Patterson.

Regarding claim **12**, Matsui in view of Muratani disclose "**A method as claimed in claim 11**," but does not specifically disclose "**characterized in that the communication of the control device with the at least one encryption/decryption means and/or the at least one rounding key generation means takes place by means of at least one handshake protocol**."

However, Hennessy and Patterson disclose an asynchronous bus wherein "self-timed, handshaking protocols are used between bus sender and receiver" (Page 499, Par. 2, lines 1-2).

Hennessy and Patterson, Matsui, and Muratani are analogous art because they are in the same field of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui in view of Muratani by using handshake protocol as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to

lengthen the bus without worrying about clock skew or synchronization problems (Hennessy and Patterson, Page 499, Par. 3, lines 1-3).

Regarding claim **13**, Matsui in view of Muratani disclose "**A method as claimed in claim 11**," but does not specifically disclose "**characterized in that the communication of the control device with the at least one encryption/decryption means and the at least one rounding key generation means takes place asynchronously.**"

However, Hennessy and Patterson disclose an asynchronous bus wherein "self-timed, handshaking protocols are used between bus sender and receiver" (Page 499, Par. 2, lines 1-2).

Hennessy and Patterson, Matsui, and Muratani are analogous art because they are in the same field of computer architecture and data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui in view of Muratani by including an asynchronous bus as described by Hennessy and Patterson since it would be much easier to accommodate a variety of devices and to lengthen the bus without worrying about clock skew or synchronization problems (Hennessy and Patterson, Page 499, Par. 3, lines 1-3).

19. Claim **14** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Muratani, and further in view of Tran.

Matsui in view of Muratani discloses "**A method as claimed in claim 11**," but does not specifically disclose "**characterized in that access to the at least one storage means takes place by means of at least one rotating pointer**."

However, Tran discloses a rotating pointer buffer for storing data in integrated circuits wherein a head pointer and a tail pointer are used to provide access (Col. 1, lines 51, 54-47, Fig. 1).

Tran, Matsui, and Muratani are analogous art because they are in the same field of endeavor of computer architecture and data storage.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify data communication system with a data scrambling of Matsui in view of Muratani by including at least one rotating pointer to provide access to storage areas in selectors as described by Tran since rotating pointer structure is superior to shifting structure in terms of lowest area consumption and speed (Tran, Col. 2, lines 18-20, Table 1).

20. Claim **17** is rejected under 35 U.S.C. 103(a) as being unpatentable over Matsui in view of Muratani and further in view of Verbauwhede.

For examining purposes, claim **17** will be considered to be dependent on claim **11**. Matsui in view of Muratani discloses "**A method as claimed in claim 11**," but does not specifically disclose "**characterized in that it is embodied as a method of AES calculation using an AES coprocessor as claimed in claim 10**."

However, Verbauwhede discloses AES architecture for encrypting or decrypting data (Col. 1, Par. 0007, line 1).

Verbauwhede, Matsui, and Muratani are analogous art because they are in the same field of endeavor of data encryption/decryption.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the data communication system with a data scrambling of Matsui in view of Muratani to be an AES implementation as described by Verbauwhede for the purpose of achieving a high data rate (Verbauwhede, Col. 1, Par. 0006, lines 1-2).

Conclusion

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TN

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148